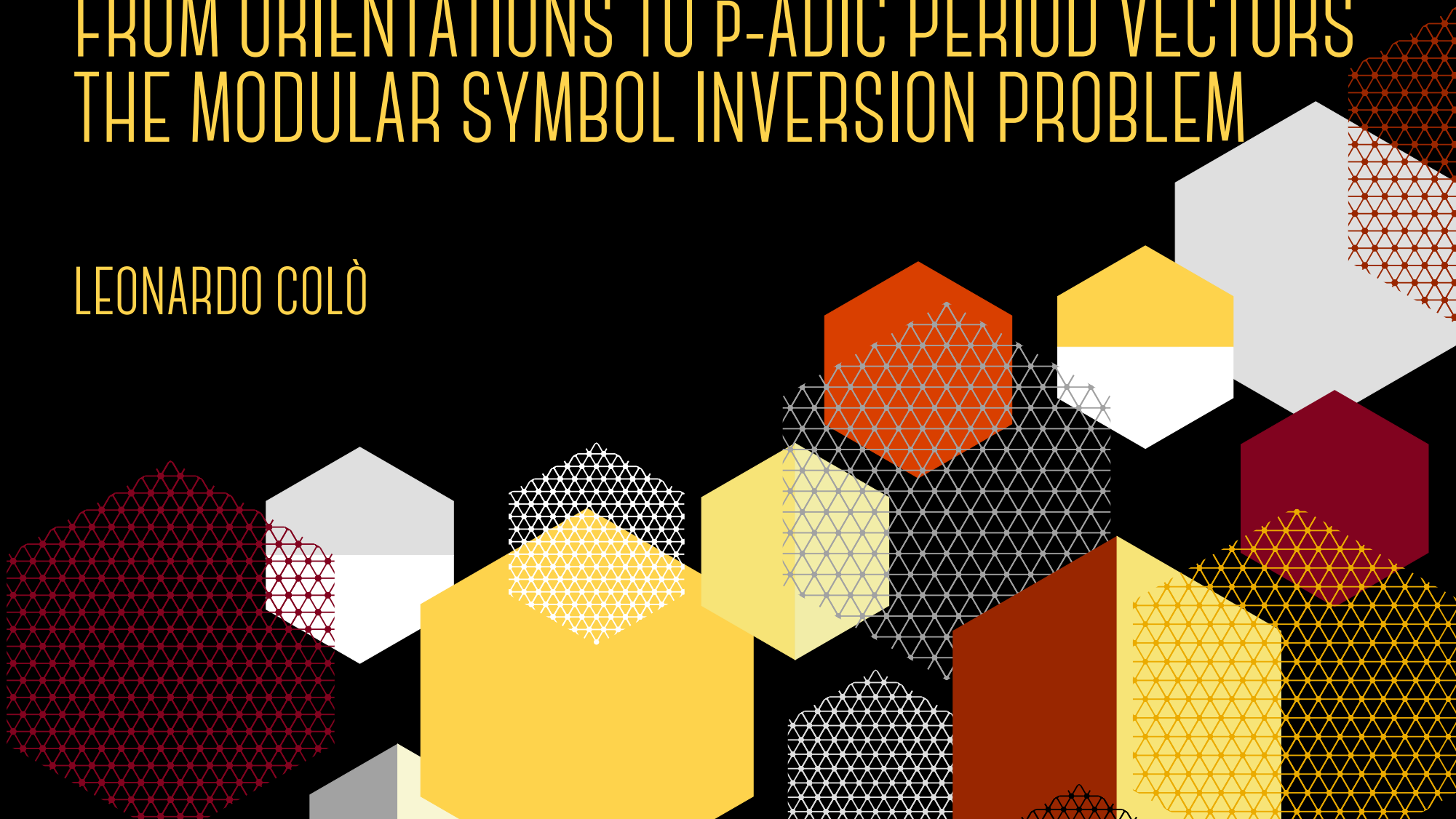
Marseille, 11 December, 2025

SEMINAIRE I2M

UNIVERSITY OF WATERLOO

FROM ORIENTATIONS TO p-ADIC PERIOD VECTORS THE MODULAR SYMBOL INVERSION PROBLEM

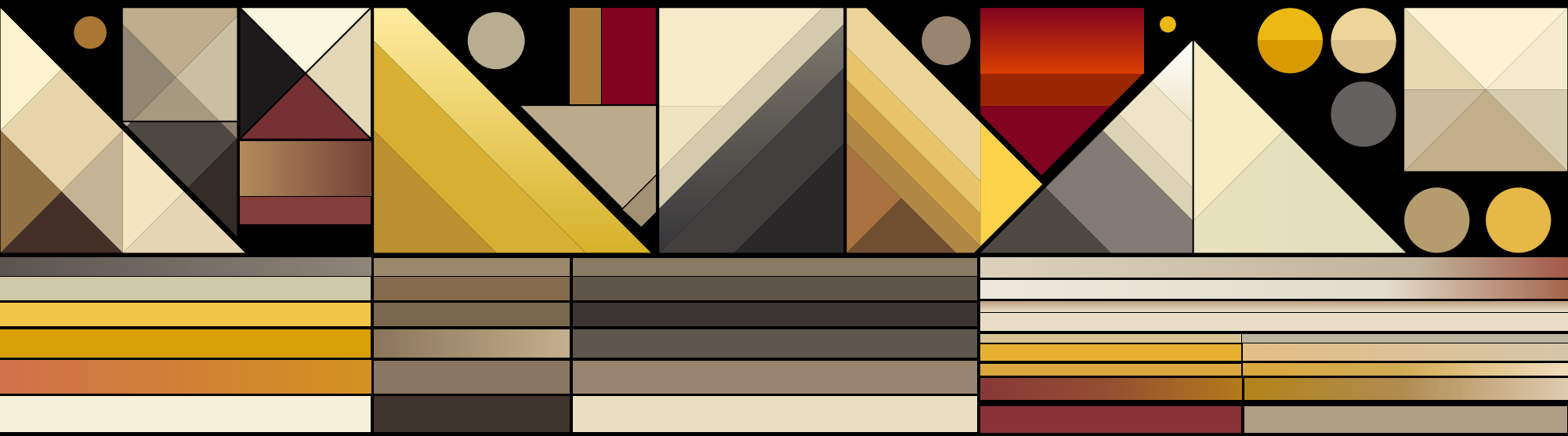
LEONARDO COLÒ



CONTENTS

- Supersingular isogeny graphs.
- Bruhat-Tits trees.
- Modular curves and level structures.
- Attaching modular symbols to orientations.
- p-adic integrals.
- Cryptographic constructions.

SUPERSINGULAR ELLIPTIC CURVES & ORIENTATIONS



L.COLÒ UWAT

Elliptic curves

An elliptic curve over a field k (char $\neq 2, 3$):

$$E : y^2 = x^3 + Ax + B, \qquad \Delta = 4A^3 + 27B^2 \neq 0.$$

- Isogeny: non-constant algebraic group morphism $\varphi : E_1 \to E_2$.
- Kernel-theorem: if $\gcd(\deg \varphi, \mathrm{char}(k)) = 1$, then φ is uniquely determined by finite subgroup $\ker \varphi$.
- Dual isogeny and degree multiplication formula: $\widehat{\varphi} \circ \varphi = [\deg \varphi]$.

ISOGENY GRAPHS

Definition

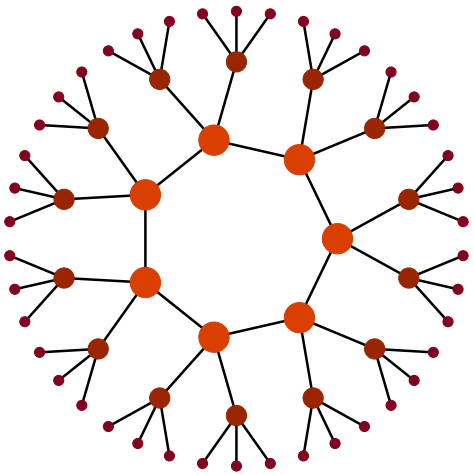
Given an elliptic curve E over k, and a finite set of primes S, we can associate an isogeny graph $G_S(E)$

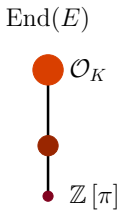
- whose vertices are elliptic curves isogenous to E over $\bar{k}$, and
- whose edges are isogenies of degree $\ell \in S$.

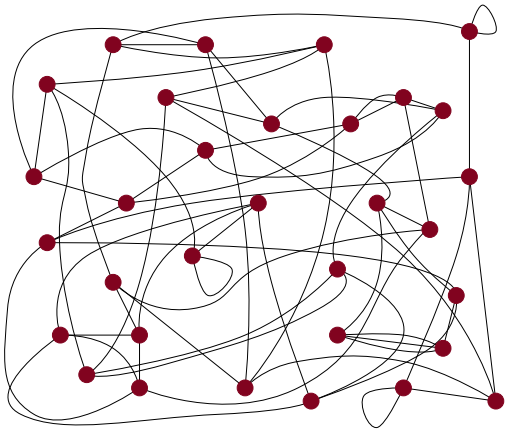
If $S = \{\ell\}$, then we write $G_\ell(E)$, the ℓ-isogeny graph.

The vertices are defined up to $\bar{k}$-isomorphism and the edges from a given vertex are defined up to a $\bar{k}$-isomorphism of the codomain.

The ℓ-isogeny graph of E is $(\ell + 1)$-regular (as a directed multigraph).







ORDERS AND ORIENTATIONS

Let E/k be a supersingular elliptic curve over $k = \mathbb{F}_{p^2}$, let K be an imaginary quadratic field with maximal order $\mathcal{O}_K$, and define

$$\mathrm{End}^0(E) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}.$$

Then $\mathrm{End}^0(E)$ is a quaternion algebra over $\mathbb{Q}$, ramified at p, which admits an embedding of K if and only if p is ramified or inert in K.

Definition

A *K-orientation* on an elliptic curve E/k is a homomorphism

$$\iota : K \hookrightarrow \mathrm{End}^0(E).$$

An *$\mathcal{O}$-orientation* on E is a K-orientation such that $\iota(\mathcal{O})$ is contained in $\mathrm{End}(E)$. An $\mathcal{O}$-orientation is *primitive* if

$$\iota : \mathcal{O} \to \iota(K) \cap \mathrm{End}(E)$$

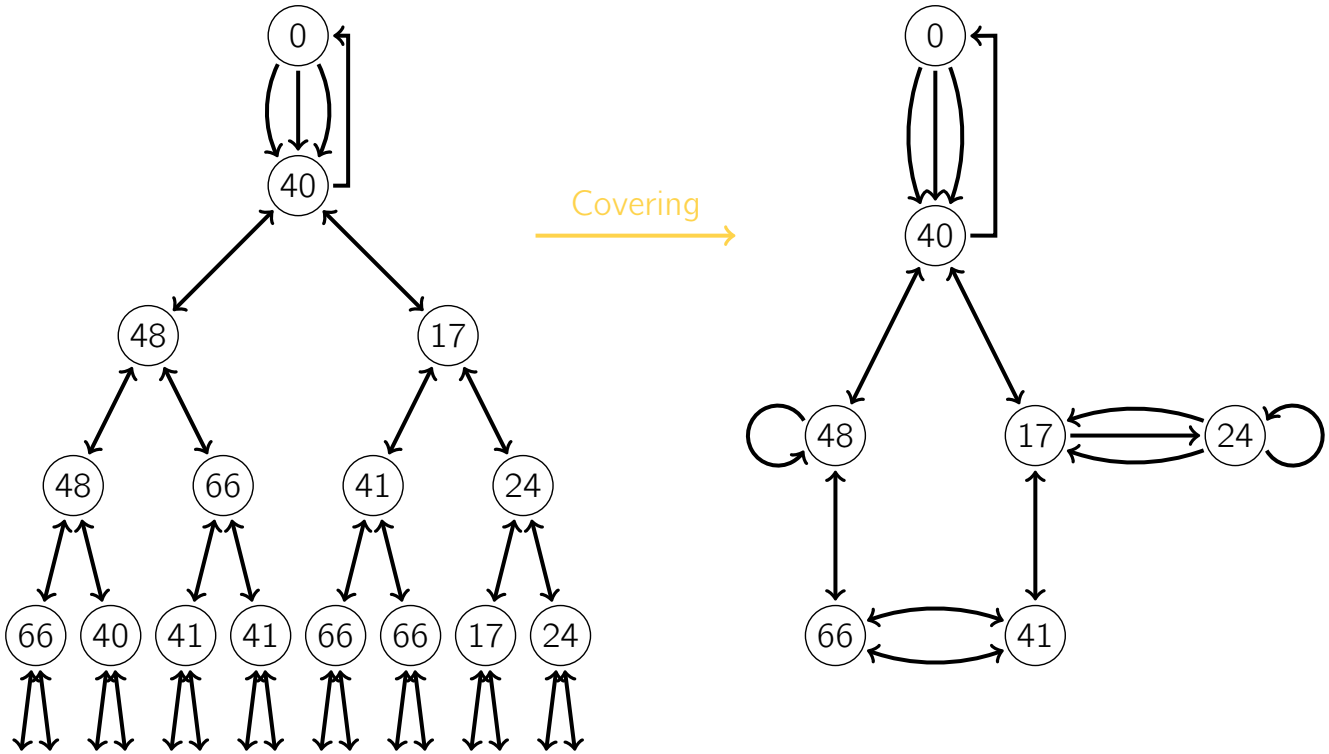
is an isomorphism.

IDEAL CLASSES AND ORIENTED SUPERSINGULAR CURVES

L.COLÒ UWAT

Theorem

The category of K-oriented supersingular elliptic curves (E, ι), whose morphisms are isogenies commuting with the K-orientations, is equivalent to the category of elliptic curves with CM by K.



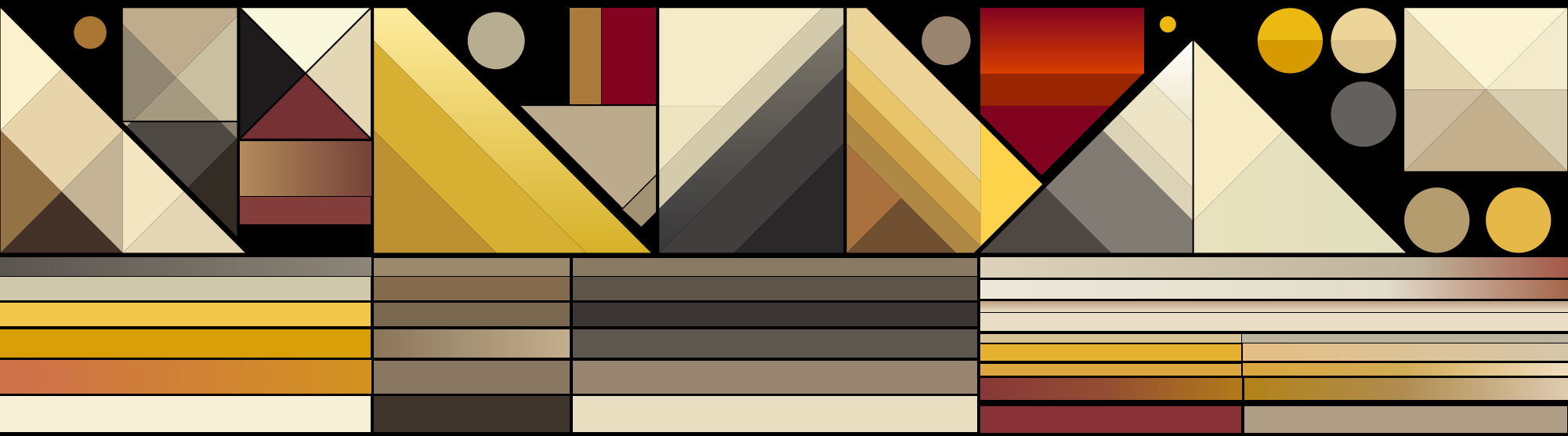
Definition

Let E be a supersingular elliptic curve, and let for a prime $\ell \neq p$ we define the ℓ-adic Tate module:

$$T_\ell(E) = \varprojlim E[\ell^n] \cong \mathbb{Z}_\ell^2.$$

- Every endomorphism of E acts $\mathbb{Z}_\ell$-linearly on $T_\ell(E)$.
- $\ell \neq p$: good reduction $\Rightarrow$ $T_\ell(E)$ free rank 2.
- Ideal classes act as elements of $\mathrm{GL}_2(\mathbb{Z}_\ell)$.
- An optimal embedding $\iota : \mathcal{O} \to \mathrm{End}(E)$ induces an action of $\mathcal{O}$ on $T_\ell(E)$. Thus the data of an oriented supersingular curve (E, ι) determines a $\mathcal{O}$-stable lattice in $V_\ell(E) = T_\ell \otimes \mathbb{Q}$, and horizontal isogenies preserve this lattice structure.

SUPERSINGULAR ISOGENY GRAPHS & BRUHAT-TITS TREE



THE BRUHAT-TITS TREE

L.COLÒ UWAT

Definition

The Bruhat-Tits tree associated to $\mathrm{PGL}_2(\mathbb{Q}_\ell)$ is the graph $\mathcal{B}_\ell$ such that

- homothety classes of lattices of $\mathbb{Q}_\ell^2$.
- edges represent set of pairs of adjacent homothety classes.

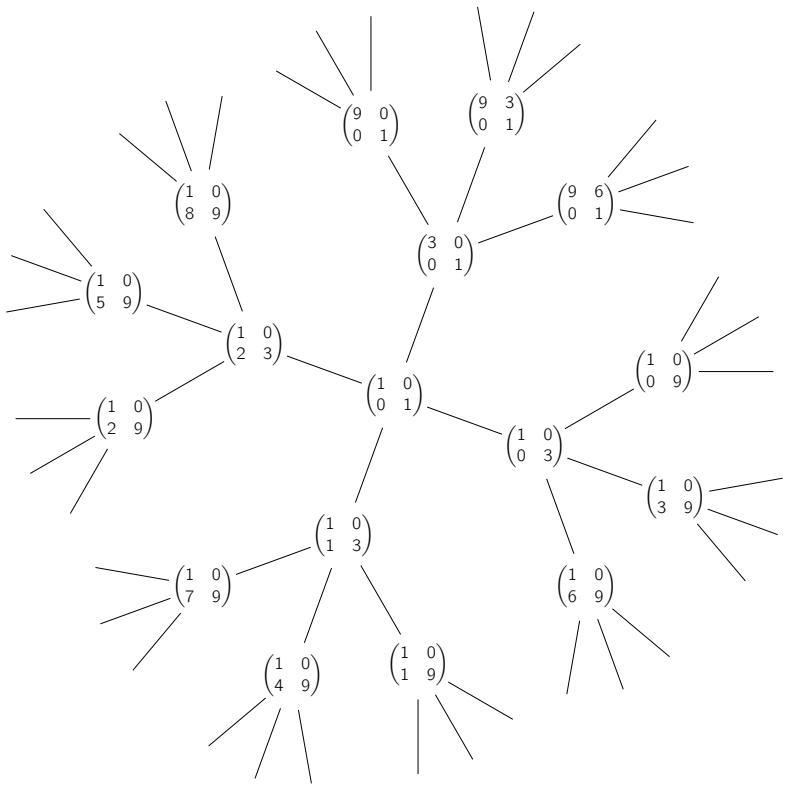
- A lattice L of $\mathbb{Q}_\ell^2$ is a free $\mathbb{Z}_\ell$-module of rank 2 in $\mathbb{Q}_\ell^2$
- We say that two lattices L_1 and L_2 are homothetic if there exists $\lambda \in \mathbb{Q}_\ell^\times$ such that $L_1 = \lambda L_2$.
- Two homothety classes $[L_1]$ and $[L_2]$ are adjacent if their representatives L_1 and L_2 can be chosen so that $\ell L_1 \subset L_2 \subset L_1$.

$\mathcal{B}_\ell$ is an Infinite $(\ell+1)$-regular tree encoding lattices in $\mathbb{Q}_\ell^2$.

THE BRUHAT-TITS TREE - EXAMPLE

There are several equivalent ways to define $\mathcal{B}_\ell$

- homothety classes of lattices of $\mathbb{Q}_\ell^2$.
- classes of matrices in $\mathrm{PGL}_2(\mathbb{Q}_\ell)/\mathrm{PGL}_2(\mathbb{Z}_\ell)$.
- maximal orders in the quaternion algebra $M_2(\mathbb{Q}_\ell)$.



ORIENTED VERTICES

- Let $\mathcal{B}_\ell$ be denote the Bruhat-Tits tree of $\mathrm{PGL}_2(\mathbb{Q}_\ell)$.
- Let $\Gamma = R$, where $R = \mathrm{End}(E_0)$ is a fixed maximal order. Then Γ acts on $\mathcal{B}_\ell$ without inversion, and the quotient $\Gamma\backslash\mathcal{B}_\ell$ is a finite graph, canonically identified with the $\overline{\mathbb{F}}_p$-isogeny graph of supersingular elliptic curves.
- Let (E, ι) be a supersingular elliptic curve equipped with an embedding

$$\iota : \mathcal{O} \hookrightarrow \mathrm{End}(E).$$

This induces an $\mathcal{O} \otimes \mathbb{Z}_\ell$-module structure on the ℓ-adic Tate module:

$$T_\ell(E) \cong \mathbb{Z}_\ell^2, \qquad \iota(a) \cdot v \in T_\ell(E) \text{ for all } a \in \mathcal{O}.$$

A vertex in $\mathcal{T}_\ell$ now carries **additional information**:

$$(E, \iota) \quad \longleftrightarrow \quad [T_\ell(E), \text{ with its full order structure } \mathcal{O} \otimes \mathbb{Z}_\ell].$$

No vertices or edges disappear — instead, the tree becomes a **decorated tree** where each vertex encodes the conductor profile.

IDEAL CLASSES AS ORIENTED PATHS

Let (E_0, ι_0) be a fixed oriented supersingular curve and let $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$ be an ideal class, with $\mathfrak{a}$ coprime to $p\ell$.

- Fix a basis of the ℓ-adic Tate module $T_\ell(E_0) = \langle P, Q \rangle \cong \mathbb{Z}_\ell^2$.
- The induced map on Tate modules is an automorphism $T_\ell(\phi_\mathfrak{a}) : T_\ell(E_0) \to T_\ell(E_\mathfrak{a})$ represented by a matrix

$$M_\mathfrak{a} \in \mathrm{GL}_2(\mathbb{Z}_\ell)$$

  in the basis (P, Q).
- For each $n \geq 1$, the reduction of $M_\mathfrak{a}$ modulo ℓ^n describes the action on the finite module $E_0[\ell^n] \cong (\mathbb{Z}/\ell^n\mathbb{Z})^2$.

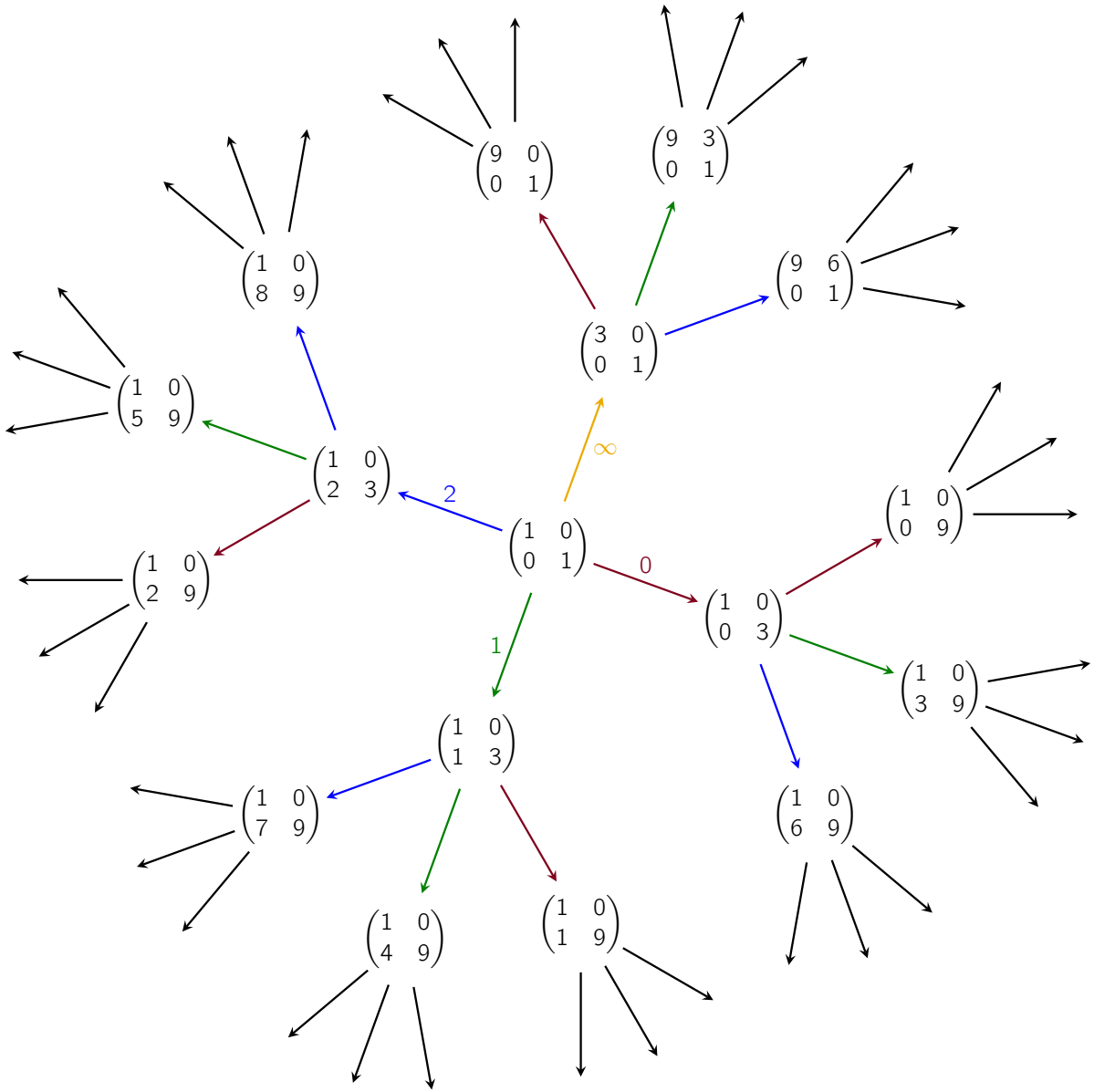
The sequence of digits

$$(c_0, c_1, c_2, \dots)$$

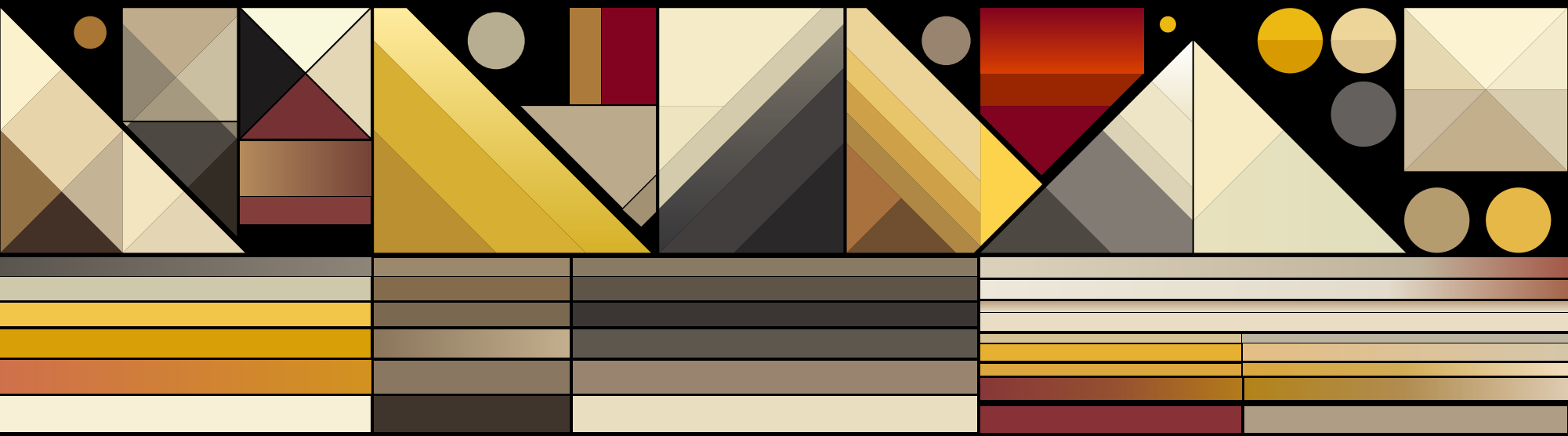
encodes a unique non-backtracking path in the Bruhat–Tits tree $\mathcal{T}_\ell$ starting at the vertex of (E_0, ι_0). Thus an ideal class $[\mathfrak{a}]$ determines a **canonical oriented path**

$$[\mathfrak{a}] \longleftrightarrow \text{ geodesic walk in } \mathcal{T}_\ell \text{ from } (E_0, \iota_0) \text{ to } (E_\mathfrak{a}, \iota_\mathfrak{a}).$$

NAVIGATING THE BRUHAT-TITS TREE - EXAMPLE



MODULAR SYMBOLS AND RELATIVE HOMOLOGY



MODULAR GROUP

The group

$$\mathrm{SL}_2(\mathbb{Z}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \,\middle|\, ad - bc = 1 \right\}$$

acts by fractional linear Mobius transformations

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \cdot \tau = \frac{a\tau + b}{c\tau + d}$$

on the upper half plane

$$\mathbb{H} = \{ z \in \mathbb{C} \,|\, \mathrm{Im}(z) > 0 \}$$

equipped with its standard complex analytic structure.

We define the modular group as the quotient group

$$\Gamma(1) = \mathrm{SL}_2(\mathbb{Z})/\{\pm I\}$$

CONGRUENCE SUBGROUPS

We define the principal congruence subgroup as the kernel of the reduction map $\mathrm{SL}_2(\mathbb{Z}) \to \mathrm{SL}_2(\mathbb{Z}/N\mathbb{Z})$. This is

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

A subgroup Γ of $\mathrm{SL}_2(N)$ is called a congruence subgroup if it contains $\Gamma(N)$ for some N. Some important examples of congruence subgroups are

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \bmod N \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \,\middle|\, \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \bmod N \right\}$$

MODULAR FORMS AND CUSP FORMS OF WEIGHT 2

A holomorphic function $f : \mathfrak{H} \to \mathbb{C}$ is a *weight-2 modular form* for $\Gamma_0(N)$ if

$$f(\gamma z)\,(cz+d)^{-2} = f(z) \qquad \text{for all } \gamma = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N),$$

and f is holomorphic at the cusps.

The space of such forms is denoted $M_2(\Gamma_0(N))$.

A form $f \in M_2(\Gamma_0(N))$ is a *cusp form* if in its q-expansion at every cusp, the constant term vanishes. The subspace of cusp forms is denoted $S_2(\Gamma_0(N))$. To every $f \in S_2(\Gamma_0(N))$ we attach a differential

$$\omega_f = f(z)\,dz,$$

which is holomorphic on the modular curve $X_0(N)$.

HECKE OPERATORS ON MODULAR FORMS

L.COLÒ UWAT

For each integer $n \geq 1$, the *Hecke operator* T_n acts on $M_2(\Gamma_0(N))$ and $S_2(\Gamma_0(N))$ via double coset correspondences. When $(n, N) = 1$, one has the formula

$$T_n(f)(z) = n \sum_{\substack{ad=n \\ 0 \leq b < d}} d^{-2} \, f\left(\frac{az+b}{d}\right).$$

These operators commute, are normal with respect to the Petersson inner product, and preserve $S_2(\Gamma_0(N))$. They play a central role in linking analytic and arithmetic constructions.

THE MODULAR CURVE $X_0(N)$ AND ITS CUSPS

Let $\Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z})$ be the congruence subgroup of level N defined by

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) : c \equiv 0 \pmod{N} \right\}.$$

The modular curve $X_0(N)$ is the compact Riemann surface (and smooth projective algebraic curve over $\mathbb{Q}$) obtained by compactifying the quotient

$$Y_0(N) = \Gamma_0(N) \backslash \mathbb{H}$$

by adding finitely many cusps C, corresponding to the $\Gamma_0(N)$-orbits in $\mathbb{P}^1(\mathbb{Q})$. We denote by $g = g(X_0(N))$ the genus of $X_0(N)$ and by

$$C = \{c_1, \ldots, c_c\}$$

the finite set of cusps, where $c = \#C$.

RELATIVE HOMOLOGY & MANIN SYMBOLS

We let H denote the relative homology group

$$H := H_1(X_0(N), C; \mathbb{Z}).$$

Let Δ be the free abelian group on formal symbols $\{r \to s\}$ with $r, s \in \mathbb{P}^1(\mathbb{Q})$, modulo the relations

$$\{r \to s\} + \{s \to t\} + \{t \to r\} = 0 \qquad \text{for all } r, s, t \in \mathbb{P}^1(\mathbb{Q}),$$
$$\{r \to r\} = 0 \qquad \text{for all } r \in \mathbb{P}^1(\mathbb{Q}).$$

The group $\Gamma_0(N)$ acts on Δ by

$$\gamma \cdot \{r \to s\} := \{\gamma r \to \gamma s\}.$$

Proposition

There is a natural isomorphism of abelian groups

$$H_1(X_0(N), C; \mathbb{Z}) \cong \Delta_{\Gamma_0(N)},$$

where $\Delta_{\Gamma_0(N)} := \Delta / \langle \gamma \cdot x - x : \gamma \in \Gamma_0(N), x \in \Delta \rangle$

RANK FORMULA

The rank of the relative homology H can be expressed in terms of the genus and the number of cusps.

proposition

Let $g = g(X_0(N))$ be the genus of $X_0(N)$ and let $c = \#C$ be the number of cusps. Then

$$\operatorname{rank}_{\mathbb{Z}} H_1(X_0(N), C; \mathbb{Z}) = 2g + (c - 1).$$

Note that $\#C = \sum_{b|N} \varphi\left(\gcd\left(b, \frac{N}{b}\right)\right)$

HECKE OPERATORS ON MODULAR SYMBOLS

The Hecke algebra $\mathbb{T}$ of level $\Gamma_0(N)$ is generated by the usual Hecke operators T_ℓ for primes $\ell \nmid N$ and U_ℓ for $\ell \mid N$.

These operators act on cusp forms of weight 2 and level $\Gamma_0(N)$, but also on the homology H via correspondences on $X_0(N)$.

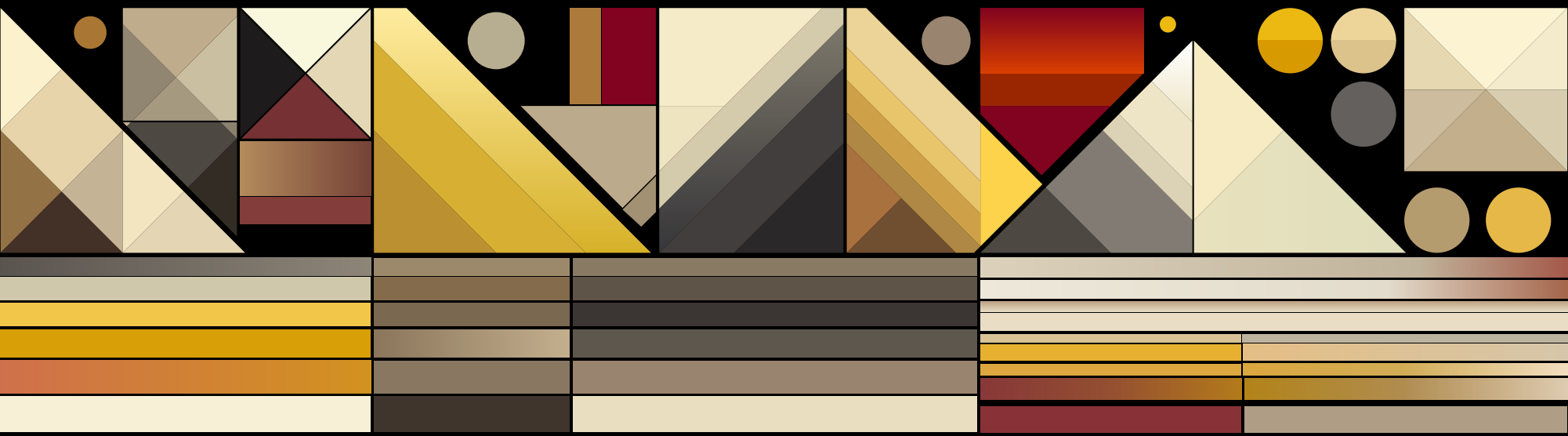
$$T_\ell \{\alpha \to \beta\} = \begin{pmatrix} \ell & 0 \\ 0 & 1 \end{pmatrix} \{\alpha \to \beta\} + \sum_{b=0}^{\ell-1} \begin{pmatrix} 1 & b \\ 0 & \ell \end{pmatrix} \{\alpha \to \beta\}$$

More precisely, each Hecke operator T_ℓ induces an endomorphism

$$T_\ell : H_1(X_0(N), C; \mathbb{Z}) \to H_1(X_0(N), C; \mathbb{Z}),$$

defined at the level of modular symbols by a finite linear combination of pullbacks and pushforwards along modular correspondences.

ATTACH MODULAR SYMBOL TO AN ORIENTATION



BRANDT HOMOLOGY

Input: An $\mathcal{O}$–oriented supersingular elliptic curve (E_0, ι_0) and an ideal class $[\mathfrak{a}] \in \mathrm{Pic}(\mathcal{O})$.

- Supersingular curves with orientation correspond to left ideal classes in a definite quaternion algebra:

$$(E, \iota) \leftrightarrow [I] \in \mathcal{Cl}(\mathcal{O}_B).$$

- The Brandt module

$$\mathbb{B} = \mathbb{Z}[\mathcal{Cl}(\mathcal{O}_B)]$$

  carries a Hecke action.
- Via Jacquet–Langlands + Eichler–Shimura:

$$\iota_{\mathrm{JL}} : \mathbb{B} \hookrightarrow H_1(X_0(N), C; \mathbb{Z}) \otimes \mathbb{Q}.$$

- $\mathrm{Pic}(\mathcal{O})$ acts by permuting ideal classes; transporting a fixed base cycle gives:

$$\gamma^{(1)}([\mathfrak{a}]) := \rho([\mathfrak{a}])(\gamma_0) \in H_1(X_0(N), C; \mathbb{Z}).$$

GEOMETRIC GEODESIC CYCLES ON $X_0(N)$

Input: The same ideal class $[\mathfrak{a}]$.

- CM theory yields a Heegner point:

$$[\mathfrak{a}] \longmapsto x_{\mathfrak{a}} \in X_0(N)(\mathbb{C}),$$

compatible with the class group action.

- Fix:

$$x_0 := x_{\mathcal{O}_f}, \qquad c_\infty \in \text{cusps}.$$

Choose analytic paths:

$$\delta_{\mathfrak{a}} : x_{\mathfrak{a}} \to c_\infty, \qquad \delta_0 : x_0 \to c_\infty.$$

- Relative homology:

$$\gamma^{(2)}([\mathfrak{a}]) := \delta_{\mathfrak{a}} - \delta_0 \in H_1(X_0(N), C; \mathbb{Z}).$$

This is well-defined modulo absolute cycles and depends only on $[\mathfrak{a}]$.

BRUHAT-TITS GRAPH AND HARMONIC COCYCLES

Input: Same ideal class $[\mathfrak{a}]$.

- By Cerednik–Drinfeld uniformization, $X_0(N)$ admits a p-adic model whose skeleton is:

$$\Gamma \backslash \mathcal{T}_p,$$

  where $\mathcal{T}_p$ is the Bruhat–Tits tree of $\mathrm{PGL}_2(\mathbb{Q}_p)$.
- Vertices correspond to oriented supersingular curves (or their p-adic lifts).
- The class-group action induces an *oriented path*:

$$v_0 \rightsquigarrow v_{\mathfrak{a}} \quad \text{in } \Gamma \backslash \mathcal{T}_p.$$

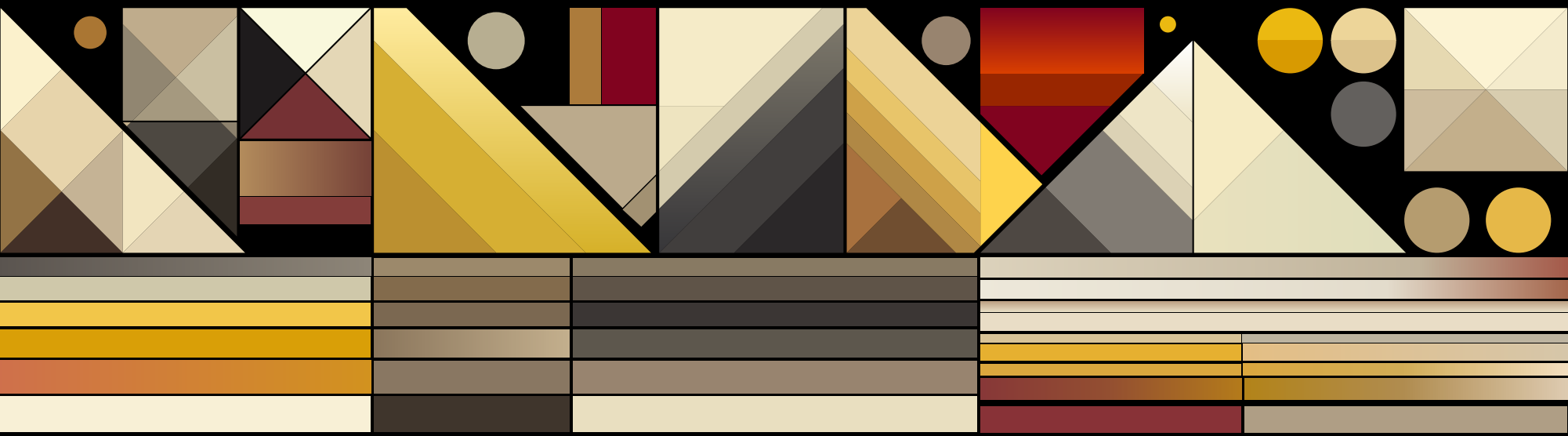
- Closing this path to a fixed base reference edge yields a graph cycle

$$c_{\mathfrak{a}} \in H_1(\Gamma \backslash \mathcal{T}_p; \mathbb{Z}).$$

- Via the harmonic cocycle isomorphism:

$$\gamma^{(3)}([\mathfrak{a}]) := \Phi(c_{\mathfrak{a}}) \in H_1(X_0(N), C; \mathbb{Z}).$$

p-ADIC PERIOD VECTORS AND COLEMAN INTEGRALS



WEIGHT-2 CUSP FORMS AND THE PERIOD PAIRING

$S_2(\Gamma_0(N))$ is the space of weight-2 cusp forms of level $\Gamma_0(N)$.

Definition

Let f be a weight-2 cusp form for $\Gamma_0(N)$. Classically, the *period pairing* between f and a homology class $\gamma \in H_1(X_0(N), C; \mathbb{Z})$ is the complex integral

$$\langle f, \gamma \rangle = \int_\gamma f(z)\, dz,$$

defined by integrating $f(z)\, dz$ along a singular 1-cycle representing γ in the upper half-plane model.

This extends linearly in both arguments and induces a perfect pairing between the cuspidal subspace of $H_1(X_0(N); \mathbb{Z})$ and the corresponding space of cusp forms.

DEFINING THE PERIOD VECTOR

Let $f_1, \ldots, f_d$ be a fixed collection of weight-2 cusp forms For $\gamma \in H$, we define the (infinite precision) p-adic period vector

$$\Pi(\gamma) := \left(\langle f_1, \gamma \rangle_p, \ldots, \langle f_d, \gamma \rangle_p\right) \in \mathbb{Q}_p^d.$$

Definition

Let q be a prime distinct from p and not dividing N. For $m \geq 1$ and $\gamma \in H$, the *truncated p-adic period vector* of γ is

$$\Pi_m(\gamma) := \left(\langle f_1, \gamma \rangle_p, \ldots, \langle f_d, \gamma \rangle_p\right) \bmod p^m \in (\mathbb{Z}/p^m\mathbb{Z})^d.$$

The map $\Pi_m : H \to (\mathbb{Z}/p^m\mathbb{Z})^d$ is $\mathbb{Z}$-linear, and its image is contained in a subgroup whose size depends on d, p, and m.

p-ADIC INTEGRATION - THE PROBLEM

Is there a Theory of p-adic integration?

We cannot use the same methods that we have in $\mathbb{R}$ or in $\mathbb{C}$ because of the totally disconnected topology of rigid analytic spaces.

Theorem (Coleman)

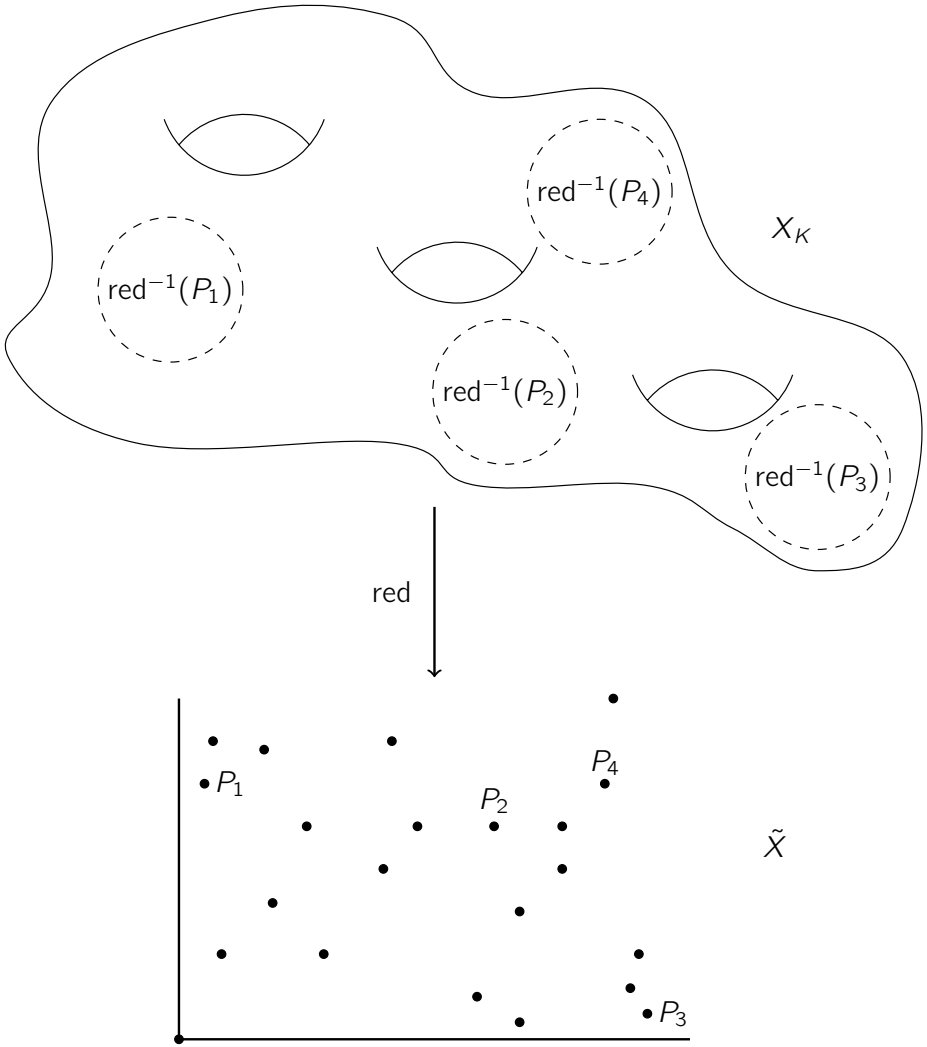
- Additivity at points: $\int_P^Q \omega + \int_Q^R \omega = \int_P^R \omega$
- Linearity on forms: $\lambda_1 \int_P^Q \omega_1 + \lambda_2 \int_P^Q \omega_2 = \int_P^Q (\lambda_1\omega_1 + \lambda_2\omega_2)$
- Change of variables: if X' is another rigid space and $\Psi : X \to X'$ is a rigid analytic map, then $\int_P^Q \Psi^*\omega' = \int_{\Psi(P)}^{\Psi(Q)} \omega'$.
- Fundamental Theorem of Calculus: $\int_P^Q df = f(Q) - f(P)$.

p-ADIC INTEGRATION - SETUP

- Let us consider a curve with good reduction.
- There is a natural reduction map

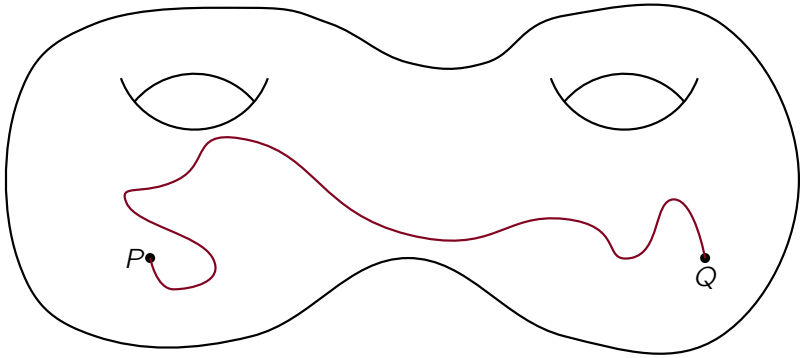
$$X \longrightarrow \tilde{X}(\mathbb{F})$$
$$x \longrightarrow \tilde{x} = x \cap A_0(X) \mod \mathfrak{p} A_0(X)$$

- The pre-image of any point of $\tilde{X}$ is a subspace of X_K isomorphic to an open unitary disk (residue disks).



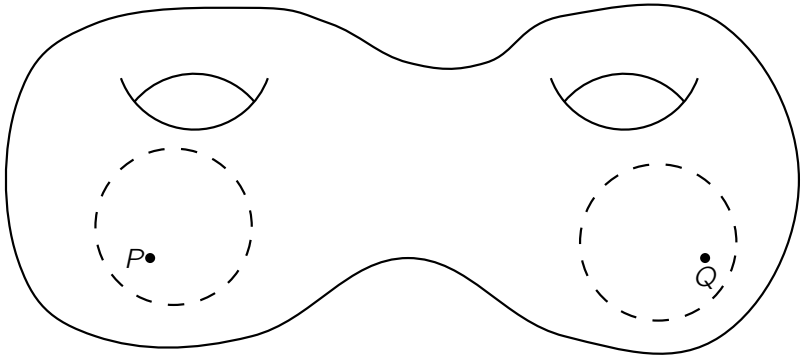
COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.



COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.

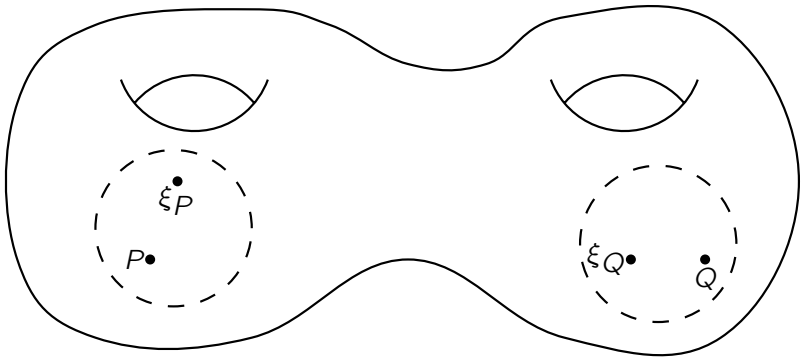


Coleman's Solution

- Cover the Affinoid space by residue disks.
- Integrate on each residue disk.
- **Problem:** Residue disks have no intersection.
- Connect integrals on different residue disks using Frobenius.

COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.



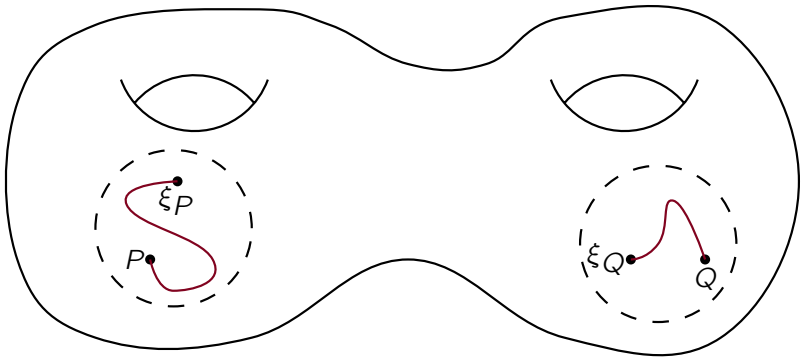
Coleman's Solution

- Find Teichmüller points

$$\int_P^Q \omega = \int_P^{\xi_P} \omega + \int_{\xi_P}^{\xi_Q} \omega + \int_{\xi_Q}^{Q} \omega$$

COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.



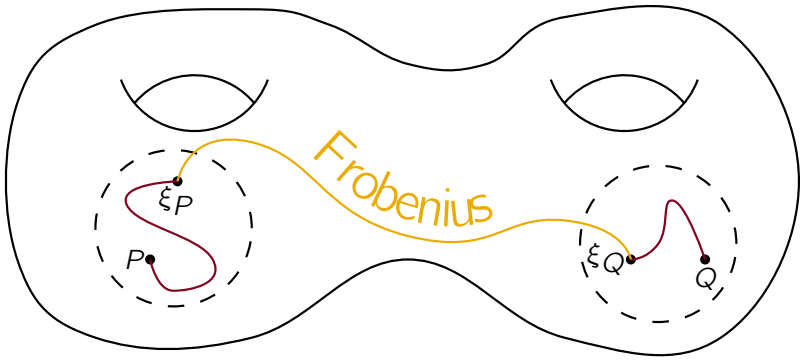
Coleman's Solution

- Find Teichmüller points
- Compute tiny integrals

$$\int_P^Q \omega = \int_P^{\xi_P} \omega + \int_{\xi_P}^{\xi_Q} \omega + \int_{\xi_Q}^{Q} \omega$$

COLEMAN INTEGRATION

There is no obvious way of integrating over affinoids.



Coleman's Solution

- Find Teichmüller points
- Compute tiny integrals
- Connect integrals using Frobenius

$$\int_P^Q \omega = \int_P^{\xi_P} \omega + \int_{\xi_P}^{\xi_Q} \omega + \int_{\xi_Q}^{Q} \omega$$

COMPUTING INTEGRALS ON $X_\emptyset(N)$

L.COLÒ UWAT

Computing $\int_Q^R \omega$ for $Q, R \in X = X_0(N)$ and $\omega \in H^0(X, \Omega^1)$

We can leverage the existence of Hecke operators.

Algorithm (Chen, Kedlaya, Lau)

- Write $\int_Q^R \omega$ as a sum of tiny integrals.
- Find a basis of holomorphic 1-forms and a suitable uniformizer.
- Compute the action of Hecke operators on cusp forms and points
- Write 1-forms as a power series in the uniformizer. This involves algebraic approximation after solving a system of equations over $\mathbb{C}$.
- Formally integrate and evaluate at the end points.

BREAKING INTO TINY INTEGRALS

Let $X/\mathbb{Q}$ be a modular curve associated to a congruence subgroup Γ.

- The Hecke operator T_p, acts on the weight 2 cusp forms, which correspond to the holomorphic 1-forms:

$$T_p^* \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix} = A \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix}$$

BREAKING INTO TINY INTEGRALS

Let $X/\mathbb{Q}$ be a modular curve associated to a congruence subgroup Γ.

- Since the Hecke operators are linear, integrating between the points Q and R gives:

$$\begin{pmatrix} \int_R^Q T_p^* \omega_1 \\ \vdots \\ \int_R^Q T_p^* \omega_g \end{pmatrix} = A \begin{pmatrix} \int_R^Q \omega_1 \\ \vdots \\ \int_R^Q \omega_g \end{pmatrix}$$

BREAKING INTO TINY INTEGRALS

Let $X/\mathbb{Q}$ be a modular curve associated to a congruence subgroup Γ.

- Since the Hecke operators are linear, integrating between the points Q and R gives:

$$\begin{pmatrix} \int_R^Q T_p^*\omega_1 \\ \vdots \\ \int_R^Q T_p^*\omega_g \end{pmatrix} = A \begin{pmatrix} \int_R^Q \omega_1 \\ \vdots \\ \int_R^Q \omega_g \end{pmatrix}$$

- For any $\omega \in H^0(X, \Omega^1)$ we obtain

$$\int_Q^R T_p^*\omega = \int_{T_p^*(Q)}^{T_p^*(R)} \omega = \sum_{i=0}^{p} \int_{R_i}^{Q_i} \omega$$

BREAKING INTO TINY INTEGRALS

Let $X/\mathbb{Q}$ be a modular curve associated to a congruence subgroup Γ.

- Since the Hecke operators are linear, integrating between the points Q and R gives:

$$\begin{pmatrix} \int_R^Q T_p^*\omega_1 \\ \vdots \\ \int_R^Q T_p^*\omega_g \end{pmatrix} = A \begin{pmatrix} \int_R^Q \omega_1 \\ \vdots \\ \int_R^Q \omega_g \end{pmatrix}$$

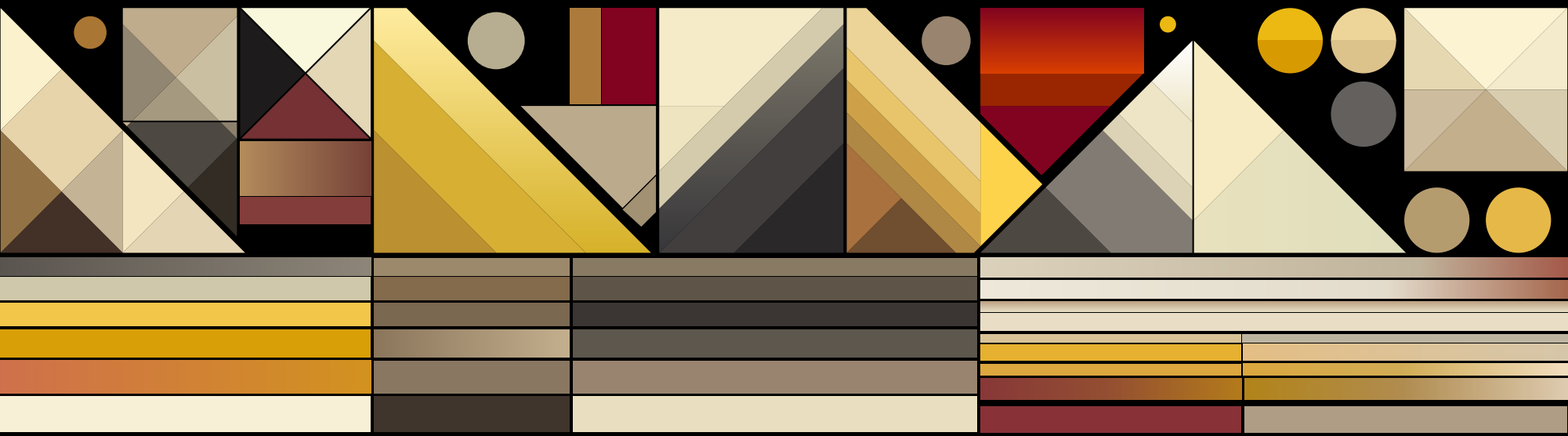
- For any $\omega \in H^0(X, \Omega^1)$ we obtain

$$\int_Q^R T_p^*\omega = \int_{T_p^*(Q)}^{T_p^*(R)} \omega = \sum_{i=0}^{p} \int_{R_i}^{Q_i} \omega$$

- We have the following fundamental equation

$$((p+1)I - A) \begin{pmatrix} \omega_1 \\ \vdots \\ \omega_g \end{pmatrix} = \begin{pmatrix} \sum_{i=0}^p \int_{Q_i}^Q \omega_1 - \sum_{i=0}^p \int_{R_i}^R \omega_1 \\ \vdots \\ \sum_{i=0}^p \int_{Q_i}^Q \omega_g - \sum_{i=0}^p \int_{R_i}^R \omega_g \end{pmatrix}$$

THE MODULAR SYMBOL INVERSION PROBLEM MSI



PATH-ENCODED HOMOLOGY CLASSES

In practice, we work with homology classes arising from combinatorially simple "paths" in a suitable graph.

We assume that there is a distinguished finite generating set $\mathcal{S} = \{\sigma_1, \ldots, \sigma_r\}$ of H over $\mathbb{Z}$, where each σ_i corresponds to an "elementary step" in such a graph.

A *path of length* L is then an expression

$$\gamma = \sigma_{i_1} + \cdots + \sigma_{i_L},$$

subject to local constraints ensuring that successive steps fit together into a valid path (e.g. edges in the Bruhat–Tits tree match up at vertices). The set of all valid paths of length at most L is denoted $\mathcal{W}_L$.

DEFINITION OF MSI

Let $\Pi_m : H \to (\mathbb{Z}/p^m\mathbb{Z})^d$ be the truncated p-adic period map. Fix parameters L, p, m, d, and consider the following relation.

MSI relation

The *Modular Symbol Inversion relation* R_{MSI} is the subset of $(\mathbb{Z}/p^m\mathbb{Z})^d \times \mathcal{W}_L$ given by

$$R_{\mathrm{MSI}} := \{(y, \gamma) : \gamma \in \mathcal{W}_L,\ y = \Pi_m(\gamma)\}.$$

We will write $(y, \gamma) \in R_{\mathrm{MSI}}$ to mean that γ is a valid "short" homology preimage of y under Π_m.

MSI problem

Given a value $y \in (\mathbb{Z}/p^m\mathbb{Z})^d$ known (or promised) to satisfy $y = \Pi_m(\gamma^\star)$ for some unknown $\gamma^\star \in \mathcal{W}_L$, the *Modular Symbol Inversion (MSI) problem* is to find a $\gamma \in \mathcal{W}_L$ such that $(y, \gamma) \in R_{\mathrm{MSI}}$.

A FIAT-SHAMIR SIGNATURE BASED ON MSI

Public parameters:

$$(p, m, N, q), \quad \Pi_m : H_1(X_0(N), C; \mathbb{Z}) \to (\mathbb{Z}/p^m\mathbb{Z})^d.$$

Public key: $\mathbf{v} = \Pi_m(\gamma)$.
Secret key: short representative γ.

- **Commitment:** Pick random short $r \in H_1(X_0(N), C; \mathbb{Z})$, send
$$c = \Pi_m(r + \gamma).$$
- **Challenge:** Verifier samples
$$b \xleftarrow{\$} \{0, 1, \ldots, q-1\}.$$
- **Response:** Send
$$z = r + b\gamma.$$
Apply rejection sampling to ensure $\|z\|$ stays within bounds.

Verification:

$$\Pi_m(z) \stackrel{?}{\equiv} c - b \cdot \mathbf{v} \quad \text{in } (\mathbb{Z}/p^m\mathbb{Z})^d.$$

(Security relies on hardness of MSI: recovering γ from $v = \Pi_m(\gamma)$.)

NAIVE KEY EXCHANGE

Setup (public):

- Same global parameters (N, p, H', Π_m) as before.
- Same base class γ_0.

Alice picks: a secret class $\gamma_A \in H'$ and publishes:

$$v_A = \Pi_m(\gamma_A).$$

Bob picks: a secret class $\gamma_B \in H'$ and publishes:

$$v_B = \Pi_m(\gamma_B).$$

Shared key (intended):

$$K := \Pi_m(\gamma_A + \gamma_B),$$

computed as:

$$\boxed{K = v_A + v_B \pmod{p^m}},$$

using p-adic linearity of Π_m.

(Useful as a pedagogical toy model; not a secure KEX without masking, hashing, or nonlinearity.)

THANK YOU FOR THE ATTENTION